CLAIMS

1. An anti-tampering signature method for rewritable media wherein display data displayed on a rewritable medium that displays display data stored in a writeable and erasable state is certified, the method comprising:

an extraction step of extracting a characteristic quantity from image data that is generated by reading the display data according to an instruction from a certifier who has certified the display data,

a data generation step of generating encrypted data by encrypting the characteristic quantity using an encryption key paired with an identifier,

an appending step of appending the identifier and the encrypted data to the rewritable medium, and

a judgment step of obtaining the encryption key based on the identifier according to an instruction of a verifier who verifies a certificate and judging whether or not the characteristic quantity obtained by decrypting the encrypted data, and the characteristic quantity of the display data match.

2. The anti-tampering signature method for rewritable media according to claim 1, wherein, in the extraction step, a general characteristic extracted from the image data generated by reading the display data is used as the characteristic quantity.

3. An anti-tampering signature apparatus for executing an anti-tampering signature method for rewritable media wherein display data displayed on a rewritable medium that displays display data stored in a writeable and erasable state is certified, the apparatus comprising:

a characteristic quantity extraction means for extracting a characteristic quantity that represents a characteristic of image data generated by reading the display data according to an instruction from a certifier who has certified the display data,

an encryption / decryption means that generates encrypted data by encrypting the characteristic quantity using an encryption key paired with an identifier, and decrypts the encrypted data into the characteristic quantity,

an appending means for appending the identifier and the encrypted data to the rewritable medium, and

a tampering judgment means for judging whether or not the decrypted characteristic quantity and the characteristic quantity of the display data match.

4. An anti-tampering signature system wherein display data displayed on a rewritable medium that displays display data stored in a writeable and erasable state is certified, comprising:

an encryption key generating means that registers an identifier and generates an encryption key,

a storage means for storing the identifier and the encryption key,

a certifying means that supplies the encryption key according to a query based on the identifier, and

an anti-tampering signature apparatus provided with a characteristic quantity extraction means for extracting a characteristic quantity that represents a characteristic of image data generated by reading the display data according to an instruction from a certifier who has certified the display data, an encryption / decryption means that generates encrypted data by encrypting the characteristic quantity using an encryption key paired with an identifier, and decrypts the encrypted data into the characteristic quantity, an appending means for appending the identifier and the encrypted data to the rewritable medium, and a tampering judgment means for judging whether or not the decrypted characteristic quantity and the characteristic quantity of the display data match.

5. An anti-tampering signature program for achieving the anti-tampering signature method for rewritable media wherein display data displayed on a rewritable medium that displays display data stored in a writeable and erasable state is certified, comprising:

an extraction step of extracting a characteristic quantity from image data that is generated by reading the display data according to an instruction from a certifier who has certified the display data,

a data generation step of generating encrypted data by encrypting the characteristic quantity using an encryption key paired with an identifier,

an appending step of appending the identifier and the encrypted data to the rewritable medium, and

a judgment step of obtaining the encryption key based on the identifier according to an instruction of a verifier who verifies a certificate and judging whether or not the characteristic quantity obtained by decrypting the encrypted data, and the characteristic quantity of the display data match.

6. A computer-readable recording medium on which the anti-tampering signature program according to claim 5 is recorded.